REMARKS

The present application was filed on April 27, 2001 with claims 1-28. Claims 1-28 are currently pending in the application. Claims 1, 15, 27 and 28 are the independent claims.

In the Office Action, claims 1-6, 8-12, 14-20 and 22-28 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,257,638 to Walker et al. (hereinafter "Walker"). In addition, claims 7, 13 and 21 are rejected under U.S.C. §103(a) as being unpatentable over Walker in view of U.S. Patent No. 5,018,196 to Takaragi et al. (hereinafter "Takaragi").

Applicants respectfully traverse the §102(e) and §103(a) rejections. In addition, Applicants also choose to make a minor clarifying amendment to the independent claims. Applicants request reconsideration of the rejected claims in view of the following remarks.

With respect to the §102(e) rejection, Applicants initially note that the Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §2131, specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Claim 1 as originally filed sets forth:

A method for performing secure information processing operations utilizing a plurality of processing devices, the method comprising the steps of:
performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of the processing devices;
initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure;
receiving as part of the interaction response information from the second processing device associated with the second participant; and

11

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information;

wherein the interaction is configured such that transcripts of the interaction can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction.

In formulating the rejection of this claim, the Examiner argues that each and every element of the claim is described by Walker. More specifically, the Examiner argues that the portions of the claim beginning with "initiating" and "sending" are anticipated by Walker at col. 5, line 56 through col. 6, line 20; col. 9, lines 41-59; and col. 12, line 56 through col. 13, line 10 (Office Action, p. 3). For completeness, these portions of Walker are reproduced here.

Walker, col. 5, line 56 through col. 6, line 20 states:

The wagering establishment has a host computer with software containing a banking program which enables players to purchase, accumulate and redeem gambling credit at remote locations, even if no on-line communications exist with the gaming computer, and an audit program for recording such transactions. This may be accomplished, in one preferred embodiment of the invention, by communicating a plurality of authenticatable messages between the gaming computer and the host computer, which messages are respectively read and authenticated by each device, either through oral communications between the player and the wagering establishment, e.g., such as via an automated public telephone network having interactive voice capabilities using a touch-tone phone. The words "authenticatable", and "authenticate" as disclosed and claimed herein include cryptographic protocols such as encryption and decryption, digital signatures, one-way hashes, checksums and the like. The utilization of authenticatable messages is one way to prevent a third party or a verified player from gaining unauthorized access to the system and then attempting to fraudulently obtain or redeem gambling credit and/or tamper with the game program to produce altered wagering opportunities having only a favorable outcome. Alternatively, gambling credit can be "built-in" or preinstalled on a tamper-evident or tamper-resistant module for installation on a conventional personal computer, or pre-installed on a dedicated gaming computer provided by the wagering establishment. In the off-line embodiment, the automated public telephone network or "agent" is associated with the host computer of the wagering establishment, but it is not necessary to have a direct electronic on-line connection between the gaming computer and the host computer.

Walker , col. 9, lines 41-59 states:

12

In one application, software can be provided which instructs the gaming computer 14 to read the unique magnetic characteristics, i.e., "fingerprint", of the specific disk or data storage media on which gaming software 22 is made available for installation, for the purpose of creating a unique authenticatable message to be read and authenticated by the wagering establishment 16 to reveal to the wagering establishment 16 any unauthorized duplication of, or tampering with, data on that disk or data storage media. Alternatively, a plug-in device can interface with the gaming computer disk drive to read a portion of the disk to acquire the unique magnetic characteristics of the disk, or the wagering establishment 16 can utilize the same hardware and/or software to obtain this magnetic signature and keep this information on file for use at some future time should tampering be suspected, or as a prerequisite to authorizing any gambling functions to a specific player 12, e.g., this data can be registered with or required by the wagering establishment 16 prior to allowing the player 12 to cash-out any gambling winnings

Finally, Walker, col. 12, line 56 through col. 13, line 10 states:

In the usual course of practicing the invention, FIGS. 4A-4B depict a flowchart of a representative start-up and registration sequence in an off-line embodiment which must occur prior to wagering. Player 12 first registers various personal information with the wagering establishment 16 and obtains an alphanumeric personal identification message or code 32. The wagering establishment 16 provides player 12 with gaming software 22 containing a game program 24, a banking program 26, and an audit program 27 as described above, having an associated software identification message or code 34. The gaming software 22 may be independently tested, verified and provided on data storage media in a sealed envelope by a third party. Such data storage media can include a hard disk, floppy disk, CD-ROM and the like. The wagering establishment 16 then provides an alphanumeric start-up identification message or code 33 which the player 12 enters into the gaming computer to run the gaming software 22. Optionally, the gaming computer 14 may utilize biometrics including, but not limited to, fingerprints, voiceprints, retinal-prints and the like, using an appropriate chip or recognition software, to deny access to any unauthorized user. Such hardware and/or software is known in the art.

Applicants respectfully submit that these portions of Walker do not anticipate each and every element of claim 1. In fact, Applicants find substantial differences between Walker and the claim. With respect to the portion of claim 1 beginning with "initiating," Applicants note that Walker describes the entering of startup identification information into a gaming computer associated with

13

the participant making the entry but fails to specify that communications between processing devices must be initiated by sending "designated initiation information to the second processing device . . ., the particular interaction being configured based at least in part on one or more results from a setup procedure." This forms one difference between Walker and the claim. Moreover, with respect to the portion of claim 1 beginning with "sending," Walker describes the "communicating [of] a plurality of authenticatable messages between the gaming computer and the host computer, which messages are respectively read and authenticated by each device," but recites few details as to the specific content of these messages. Consequently, Walker also does not explicitly describe that a first processing device send additional information to a second processing device "based at least in part on the received response information" from the first processing device.

What is more, with respect to the portion of claim 1 beginning with "wherein," the Examiner further argues that this portion of the claim is anticipated by Walker at col. 4, lines 10-22 and col. 6, lines 21-54 (Office Action, p. 4). Walker at col. 4, lines 10-22 states:

> It is still another object of the invention to provide a remote gaming system by which a player can wager on future public or external events of which the outcome is uncertain such as a lottery, either through an on-line connection between a gaming computer and the wagering establishment, or off-line where the player's wager is time-stamped to generate an authenticatable message, representing the player's choice of wagering elements (i.e., numbers) for a given lottery event (occurring at some time in the future) and, including, at least one of a date/time stamp or authenticated time message, player's identification code, and computer/software identification code.

One skilled in the art will recognize that this portion of Walker describes the creation of an authenticable record of a lottery wager. However, this portion of Walker, in contrast to claim 1, fails to describe "transcripts" reciting the contents of the messages sent back and forth between processing devices.

Walker at col. 6, lines 21-54 states:

> If the gaming computer is networked to the host computer, the connection may or may not serve to regulate or control the simulation of casino games on the gaming computer

14

by the gaming software. For example, the connection may serve to have the host computer keep a record or audit-trail of all or selected activities taking place at the gaming computer for purposes of additional verification or security. Alternatively, the connection may be of a controlled nature to vary the odds of a given wager based upon any of a variety of factors such as gambling duration or a progressively increasing jackpot (e.g., in a slot machine simulation). In such an on-line embodiment, security and player verification can be obtained by utilizing a stand-alone secure message generation and authentication device, such as, for example, an encryption/decryption unit of the type commonly employed in making wireless money transfers. This device generates an authenticatable verification code based upon the user's personal identification code and possibly a second code provided to the user from the host computer or stored in the stand-alone authentication device to prevent an unauthorized user from obtaining on-line access upon having stolen a user's personal identification code.

At all times, each wager by the player generates an electronic audit-trail on the gaming computer, the host computer and/or on any networked computers by recording the amount of each wager, the outcome of each gambling event and any resulting gambling earnings or losses, in an authenticatable message or a series of messages which are read and authenticated by the host computer and/or the gaming computer. The financial resolution of each wager is cumulatively tracked by the software on the gaming computer and perhaps also on any networked computers, so that the player is able to constantly monitor his or her gambling credit balance with the wagering establishment.

Here, Walker's "audit-trail" records "all or selected activities taking place at the gaming computer" or, alternatively, "the amount of each wager, the outcome of the each gambling event and any resulting gambling earnings or losses." Again, it does not describe the transcripts of claim 1. As stated before, the transcripts in claim 1 are a record of the contents of the messages sent back and forth between processing devices. The transcripts are therefore not, as the Examiner appears to suggest, records of the activities occurring at one processing device, nor merely records of wagering amounts, outcomes, earnings or losses.

Nevertheless, despite the traversal, Applicants choose to amend without prejudice the independent claims such that the wording "transcripts of the interaction" is modified to read "the information exchanged by the first and second processing devices." Applicants believe that this amendment makes no substantive change to the scope of the claims, but merely enhances clarity.

Based on the foregoing differences, Applicants respectfully submit that Walker does not describe each and every element of claim 1 and fails to anticipate claim 1 under §102(e). The elements of independent claims 15, 27 and 28 are similar to claim 1 and are rejected on the basis of
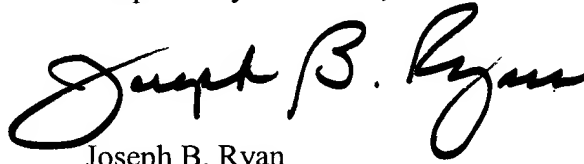
the same citations to Walker. Therefore, Applicants further submit that Walker fails to anticipate these claims. Furthermore, dependent claims 2-6, 8-12, 14-20 and 22-26 are believed allowable for at least the same reasons as their respective independent claims.

In addition, Applicants assert that many of the dependent claims contain independently patentable matter with respect to Walker. For example, the Examiner rejects claim 6 under §102(e) based on Walker at col. 8, lines 23-47 and col. 11, lines 38-50 (Office Action, p. 5). However, Walker's text and figures, unlike claim 6, contain no description of two or more players. In another example, the Examiner rejects claim 9 on the basis of Walker at col. 5, line 56 through col. 6, line 20 (Office Action, p. 6). However, unlike claim 9, Walker fails to describe a "symmetric cipher . . . having a semantic security operating in conjunction with a one-way hash function," nor does Walker describe a "commitment function." In still another example, claim 10 is rejected based on Walker at col. 4, lines 10-21 and col. 6, lines 43-54 (Office Action, p. 6). Here too, Walker fails to describe an element of the rejected claim, specifically, the configuration of the interaction such that it can handle disconnection of the parties. Finally, in a last example, the Examiner rejects claim 12 based on Walker at col. 11, lines 8-30 (Office Action, p. 7). However Walker, unlike claim 12, fails to describe the "tree structure" recited in the claim.

With respect to the §103(a) rejection of dependent claims 7, 13 and 21 over Walker in view of Takaragi, Applicants respectfully submit that the Takaragi reference fails to supplement the above-described fundamental deficiencies of Walker as applied to independent claims 1 and 15.

In view of the above, Applicants believe that claims 1-28 are in condition for allowance, and respectfully request the withdrawal of the §102(e) and §103(a) rejections.

Respectfully submitted,

Date: September 14, 2005

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517